UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,070	02/01/2002	Satyendra Yadav	P13652	2485

59796 7590 09/15/2009

INTEL CORPORATION
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
09/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,070	YADAV, SATYENDRA	
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21,22,24-28 and 31-51* is/are pending in the application.

4a) Of the above claim(s) *1-20,23,29 and 30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21,22,24-28 and 31-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21, 22, 24-28, and 31-51 are pending.

Claims 31-51 are new.

Claims 1-20, 23, and 29-30 are cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/26/2009 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 21, 22, 24-28, and 31-51 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 21, 22, 24-28, and 31-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flowers (US 6,957,348), and further in view of Naccache (US 7,168,065).

As per claim 21:

Flowers discloses a system comprising:

a network; and **(col.3, lines 55-57)**

one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations **(col.3, lines 18-23 and col.13, lines 40-45)** [*to examine a set of instructions*] embodying an invoked application to identify the invoked application **(col.3, lines 49-54 and col.7, lines 13-20),** obtain application-specific intrusion criteria, the application-specific intrusion criteria including intrusion signatures and behavior criteria **(col.6, lines 47-54 and col.8, lines 21-25)**, and monitor network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion. **(col.3, lines 45-62 and col.4, lines 4-15)**

Although, Flowers discloses operations to examine and monitor invoked applications but did not clearly discuss to examine a set of instructions.

Naccache discloses the invention for monitoring the progress in execution of a series of instructions of a computer program to analyze and verify each of the instructions has indeed been loaded or executed to the processor (col.3, lines 50-62 and col.8, lines 53-67). The monitoring device can be integrated into a programmed device which contains the

program to be monitored or into a device for executing a program to be monitored (col.6, lines 28-31).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Flowers with Naccache to examine a set of instructions embodying an invoked application to identify an invoked application because to monitor intrusion and abnormal behavior by obtaining identifiable data in each instruction set executed to verify the result of the analysis (of the instruction sets) with the reference data recorded in the program (Naccache - col.3, lines 50-62 and col.8, lines 53-67).

As per claim 22: See Flowers on col.12, lines 50-57 and Naccache on col.13, lines 15-31 ; discussing the application-specific intrusion criteria comprises a normal communication behavior threshold.

As per claim 24: See Flowers on col.3, lines 45-62 and col.4, lines 4-15; discussing to monitor network communications comprises monitoring network communications in a network intrusion detection system component running in an execution context with the invoked application.

As per claim 25: See Flowers on col.3, lines 25-30 and 50-55 and Naccache on col.10, lines 15-23; discussing the operations further comprise to provide an application-specific remedy for a detected intrusion.

As per claim 26: See Flowers on col.3, lines 50-55 and Naccache on col.7, lines 30-35; discussing to provide an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

As per claim 27: See Flowers on col.3, lines 40-55 and col.4, lines 1-30; discloses the

system of claim 24 wherein each machine further comprises a local repository and a security operation center, the security operation center includes a repository, and wherein to obtain the application specific intrusion criteria comprises to: request the application-specific intrusion criteria from a local repository; request the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository; receive the application-specific intrusion criteria from the master repository if requested; and receive the application-specific intrusion criteria from the local repository.
As per claim 28: See Naccache on col.9, lines 37-67; discussing the system of claim 24 wherein to examine the set of instructions comprises: apply a hash function to the set of instructions to generate a condensed representation; and compare the condensed representation with existing condensed representations for known applications.

As per claim 31:

Flowers discloses a detection method, comprising:

[*examining a set of instructions*] embodying an invoked application to identify the invoked application; **(col.3, lines 49-54 and col.7, lines 13-20)**

obtaining application-specific intrusion criteria, the application-specific intrusion criteria including application-specific intrusion signatures and behavior criteria; and **(col.6, lines 47-54 and col.8, lines 21-25)**

monitoring network communications for the invoked application for application- specific intrusion signatures and abnormal application behavior to detect an intrusion. **(col.3, lines 45-62 and col.4, lines 4-15)**

Although, Flowers discloses operations to examine and monitor invoked applications but did not clearly discuss to examine a set of instructions.

Naccache discloses the invention for monitoring the progress in execution of a series of instructions of a computer program to analyze and verify each of the instructions has indeed been loaded or executed to the processor (col.3, lines 50-62 and col.8, lines 53-67). The monitoring device can be integrated into a programmed device which contains the program to be monitored or into a device for executing a program to be monitored (col.6, lines 28-31).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Flowers with Naccache to examine a set of instructions embodying an invoked application to identify an invoked application because to monitor intrusion and abnormal behavior by obtaining identifiable data in each instruction set executed to verify the result of the analysis (of the instruction sets) with the reference data recorded in the program (Naccache - col.3, lines 50-62 and col.8, lines 53-67).

As per claim 32: See Naccache on col.9, lines 37-67; discussing the method of claim 31, wherein examining a set of instructions embodying an invoked application to identify the invoked application comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

As per claim 33: See Flowers on col.6, lines 47-54 and col.8, lines 21-25; discussing the method of claim 31, wherein network communications are monitored for application-specific intrusion signatures that correspond to the identified invoked application.

As per claim 34: See Flowers on col.3, lines 50-55 and Naccache on col.7, lines 30-35; discussing the method of claim 31, further comprising unloading the application-specific intrusion signatures corresponding to the identified invoked application when the identified invoked application is terminated.

As per claim 35: See Flowers on Flowers on col.12, lines 50-57 and Naccache on col.13, lines 15-31; discussing the method of claim 31, further comprising tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

As per claim 36: See Flowers on col.12, lines 50-57 and Naccache on col.13, lines 15-31; discussing the method of claim 35, wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

As per claim 37: See Flowers on col.3, lines 45-62 and col.4, lines 4-15; discussing the method of claim 35, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

As per claim 38: See Flowers on col.7, lines 11-26; discussing the method of claim 37, wherein the network intrusion detection system component and the invoked application run within a single execution context.

As per claim 39: See Flowers on col.3, lines 25-30 and 50-55 and Naccache on col.10, lines 15-23; discussing the method of claim 31, further comprising operations to provide an application-specific remedy for a detected intrusion.

As per claim 40: See Flowers on col.3, lines 45-55 and Naccache on col.10, lines 15-23; discussing the method of claim 39, wherein operations to provide an application-specific remedy for a detected intrusion comprises cutting at least a portion of the network communications for the invoked application and/or notifying a system administrator of the identified application-specific abnormal communication behavior.

As per claim 41: See Flowers col.6, lines 47-54 and col.8, lines 21-25; discussing the method of claim 31, wherein obtaining the application-specific intrusion detection signature comprises loading the application-specific intrusion detection signature from a local signature repository.

As per claim 42: See Flowers on col.3, lines 40-55 and col.4, lines 1-30; discussing the method of claim 31, wherein obtaining the application-specific intrusion detection signature comprises: requesting the application-specific intrusion detection signature from a local signature repository in communication with a remote signature repository; and receiving the application-specific intrusion detection signature from the local signature repository.

As per claim 43:

Flowers discloses the machine-readable storage medium embodying machine instructions for causing one or more processors to perform operations comprising:

[*examining a set of instructions*] embodying an invoked application to identify the invoked application; **(col.3, lines 49-54 and col.7, lines 13-20)**

obtaining application-specific intrusion criteria, the application-specific intrusion criteria including application-specific intrusion signatures and behavior criteria; and **(col.6, lines 47-54 and col.8, lines 21-25)**

monitoring network communications for the invoked application for application- specific intrusion signatures and abnormal application behavior to detect an intrusion. **(col.3, lines 45-62 and col.4, lines 4-15)**

Although, Flowers discloses operations to examine and monitor invoked applications but did not clearly discuss to examine a set of instructions.

Naccache discloses the invention for monitoring the progress in execution of a series of instructions of a computer program to analyze and verify each of the instructions has indeed been loaded or executed to the processor (col.3, lines 50-62 and col.8, lines 53-67). The monitoring device can be integrated into a programmed device which contains the program to be monitored or into a device for executing a program to be monitored (col.6, lines 28-31).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Flowers with Naccache to examine a set of instructions embodying an invoked application to identify an invoked application because to monitor intrusion and abnormal behavior by obtaining identifiable data in each instruction set executed to verify the result of the analysis (of the instruction sets) with the reference data recorded in the program (Naccache - col.3, lines 50-62 and col.8, lines 53-67).

As per claim 44: See Naccache on col.9, lines 37-67; discussing the machine-readable storage medium of claim 43, wherein examining a set of instructions embodying an invoked application to identify the invoked application comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

As per claim 45: See Flowers col.6, lines 47-54 and col.8, lines 21-25; discussing the machine-readable storage medium of claim 43, wherein network communications are monitored for application-specific intrusion signatures that correspond to the identified invoked application.

As per claim 46: See Flowers on col.3, lines 50-55 and Naccache on col.7, lines 30-35; discussing the machine-readable storage medium of claim 43, further comprising unloading the application-specific intrusion signatures corresponding to the identified invoked application when the identified invoked application is terminated.

As per claim 47: See Flowers on col.12, lines 50-57 and Naccache on col.13, lines 15-31; discussing the machine-readable storage medium of claim 43, further comprising tracking one or more characteristics of the network communications to identify application- specific abnormal communication behavior.

As per claim 48: See Flowers on col.7, lines 11-26 and col.12, lines 50-57 and Naccache on col.13, lines 15-31; discussing the machine-readable storage medium of claim 47, wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

As per claim 49: See Flowers on col.3, lines 45-62 and col.4, lines 4-15; discussing the machine-readable storage medium of claim 47, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

As per claim 50: See Flowers on col.7, lines 11-26; discussing the machine-readable storage medium of claim 49, wherein the network intrusion detection system component and the invoked application run within a single execution context.

As per claim 51: See Flowers on col.3, lines 45-55 and Naccache on col.10, lines 15-23; discussing the machine-readable storage medium of claim 43, further comprising operations to provide an application-specific remedy for a detected intrusion.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435